IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON

ALANNA C. SHORES, ANDREA L. GOWIN, and TODD W. GOWIN, on behalf of themselves and on behalf of all others similarly situated, Plaintiffs, v. PREMERA BLUE CROSS, a Washington Company, Defendant.	CASE NO.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

NOW COME Plaintiffs Alanna C. Shores, Andrea L. Gowin, and Todd W. Gowin, (collectively, "Plaintiffs") by and through their undersigned counsel, on behalf of themselves and on behalf of all others similarly situated, and hereby file this Class Action Complaint against Premera Blue Cross ("Defendant" or "Premera"). In support thereof, Plaintiffs state and allege as follows:

NATURE OF THE ACTION

1. Defendant comprises one of the largest health insurers in the Pacific Northwest, providing health care coverage to approximately 1.8 million people, primarily in Alaska and Washington. In 2013 alone, Defendant reported net income totaling approximately $7.6 billion.

2. On March 17, 2015, Premera publicly confirmed that the personal health, identification, and financial information of millions of Premera customers was improperly accessed on the IT systems of Premera (the "Data Breach") and, furthermore, that the Data

Breach extended into several of Premera's business units.[1] On its website, Premera announced that the Data Breach affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and its affiliate brands Vivacity and Connexion Insurance Solutions, Inc.[2] The Data Breach resulted in approximately 11 million individuals' information being accessed by hackers for as far back as 2002. Among the compromised data is victims' health profiles, including Social Security numbers, birthdays, emails, physical addresses, bank account information, clinical information, and detailed insurance claims.

3. Plaintiffs bring this Class Action Complaint on behalf of themselves and all other persons whose personal health, identification, and financial information was improperly obtained during the Data Breach.

4. Premera discovered the Data Breach on January 29, 2015. Premera discovered through investigation that the initial attack occurred on May 5, 2014.

5. The Data Breach could have been prevented. Three weeks before the cyberattack, auditors warned Premera that its network security procedures were inadequate.[3] Officials gave recommendations to Premera to fix its IT system inadequacies because the identified weaknesses could be exploited by hackers to expose sensitive information.[4] A few of the inadequacies were extremely basic, such as failing to implement critical patches and updates in a timely manner.[5] Premera received the auditor's report on April 18, 2014. Given the minimal effort it would have

---

[1] Home Page PREMERA, https://www.premera.com/wa/visitor/about-premera/press-releases/2015_03_17/. Unless otherwise noted, all websites cited herein were last visited on June 2, 2015.

[2] *Id*.

[3] Mike Baker, *Feds warned Premera about security flaws before breach*, THE SEATTLE TIMES (April 2, 2015) http://www.seattletimes.com/business/local-business/feds-warned-premera-about-security-flaws-before-breach/.

[4] *Id*.

[5] *Id*.

taken to fix the issues, there was more than enough time for Premera to secure its system before the May 5, 2014 data breach.

6. Premera did not have a system in place to detect that its computers had been breached. Premera discovered the Data Breach at the end of January, 2015, eight months after the cyberattack. Upon discovering the breach, Premera neglected to immediately notify the victims and delayed any notification of customers until March 17, 2015.

7. As a result of Premera's failure to protect extremely confidential data, 11 million people have been exposed to fraud and have been harmed as a result. The personal and confidential data accessed by the hackers contains everything criminals need to engage in identity theft, and to perpetrate medical care and insurance fraud, directly harming Plaintiffs and members of the Class.

8. Premera had a duty to protect the private, highly sensitive, confidential personal health, identification, and financial information of Plaintiffs and members of the Class.

9. Premera failed to reasonably and adequately safeguard its computer and information technology systems, particularly after the vulnerabilities of such systems was noted by government auditors.

10. Premera engaged in intentional misconduct in failing to rectify its susceptibility to a cyberattack even after it was told there was a problem by government auditors.

11. Premera's negligence, and violations of law and contract include: (1) failing to take adequate and reasonable measures to ensure its IT systems were protected and to safeguard the personal health, identification, and financial information of Plaintiffs and members of the Class; (2) ignoring warnings from federal government auditors that its IT systems were outdated and vulnerable; (3) failing to take available steps to prevent and stop the Data Breach from ever

happening; (4) failing to disclose to its customers the material facts that it did not have adequate IT systems and security practices to safeguard customers' personal health, identification, and financial data; and (5) failing to provide timely and adequate notice of the Data Breach. Premera's conduct has resulted in direct harm and injury to Premera insureds in the states of Washington, Alaska, Oregon, Arizona, and other states, and to consumers across the United States, as the Data Breach has also affected members of other Blue Cross Blue Shields plans who sought treatment in Washington or Alaska, as well as certain vendors.

12. Plaintiffs and the proposed Class members have a possessory interest in their personal health, identification, and financial information and an interest in it remaining private because that information, including Social Security numbers and patient identification numbers, accompanied by birth dates and addresses, has substantial value not only to Plaintiffs and the proposed Class members, but also to criminals who traffic in such information, using it to steal the identities of victims like Plaintiffs and the Class.

13. Because of the real threat of immediate harm, as well as the intrinsic value of the stolen information itself, Plaintiffs and the proposed Class members have suffered an immediate and present injury to their privacy and possessory interest as a direct result of Defendant's failure to appropriately safeguard Plaintiffs' and the proposed Class members' personal health, identification and financial information.

14. Plaintiffs and the proposed Class members have been and/or remain at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse, and have been forced to spend considerable time and money to protect themselves—and face a lifetime of constant surveillance of their financial and medical records—monitoring, loss of

rights, and potential medical problems, among other harms - as a result of Premera's conduct in failing to adequately protect their personal health, identification and financial information.

THE PARTIES

15. Plaintiff, Alanna C. Shores, is an adult individual residing in the State of Washington. Plaintiff is a citizen of the State of Washington. Plaintiff's personal health, identification, and financial information were compromised in the Data Breach.

16. Plaintiff, Andrea L. Gowin, is an adult individual residing in the State of Washington. Plaintiff is a citizen of the State of Washington. Plaintiff's personal health, identification, and financial information were compromised in the Data Breach.

17. Plaintiff, Todd W. Gowin, is an adult individual residing in State of Washington. Plaintiff is a citizen of the State of Washington. Plaintiff's personal health, identification, and financial information were compromised in the Data Breach.

18. The Class includes citizens of Alaska, Washington, Oregon and other states.

19. Defendant Premera is a citizen of the State of Washington, headquartered at 7001 220th Street SW, Building 1, Mountlake Terrace, Washington 98043.

20. Premera is one of the largest health insurers in the Pacific Northwest. Premera provides healthcare benefits primarily in Washington and Alaska, but also throughout the United States.

21. Premera reported $7.6 billion in total revenues and $2.8 billion in total assets in fiscal year 2013.

JURISDICTION AND VENUE

22. This Court has jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because: (i) the Class (as defined below) has more than 100 Class members; (ii) the

amount at issue exceeds five million dollars, exclusive of interest and costs; and (iii) at least one member of the putative class is a citizen of a state different from Defendant's state of citizen ship.

23. This Court has personal jurisdiction over Premera because Premera is authorized to do and does do business in the State of Washington.

24. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because many of the acts and transactions giving rise to this action occurred in this District and because Premera is subject to personal jurisdiction in this District.

FACTUAL BACKGROUND AND ALLEGATIONS

I. PREMERA'S COLLECTION OF PERSONAL, CONFIDENTIAL INFORMATION

25. Premera is one of the largest for-profit managed health care companies in the Pacific Northwest. It serves approximately 1.8 million people, spanning from individuals and families to Fortune 100 employer groups. Premera operates plans including Premera Blue Cross (coverage in Washington) and Premera Blue Cross Blue Shield of Alaska (coverage in Alaska).

26. Premera also participates in the BlueCard program, which is national program of the Blue Cross Blue Shield Association that enables members of one BlueCross BlueShield plan to obtain healthcare services while traveling or living in another BlueCross BlueShield service area.

27. Plaintiffs and members of the proposed Class have, or previously had, health insurance issued by Premera. Premera has either required them to provide their personal health, identification and financial information, including full legal names, dates of birth, Social Security numbers, billing information, street addresses, email addresses, employment information, income data, and highly confidential personal health history and other information

to become an insured under Premera's insurance coverage or has obtained that information from other Blue Cross/Blue Shield entities in order to provide health care coverage for non-Premera insureds.

28. Premera was, and currently is, well aware that the sensitive personal information provided to them by Class members is confidential, highly sensitive, and vulnerable to attack.

29. Plaintiffs and the proposed Class members and Defendant agreed that, as part of the health care services provided to Plaintiffs and the proposed Class Members, Defendant would protect the patient identification data of Plaintiffs and the proposed Class members.

30. Premera promised Plaintiffs and the members of the Class that they are "committed to maintaining the confidentiality of your medical and financial information, which we refer to as your 'personal information,' regardless of format: oral, written, or electronic."[6]

31. In its Notice of Privacy Practices (which all insureds receive), Premera states and represents that it has numerous procedures in place to protect the sensitive and personal information of its insureds. The Notice of Privacy Practices appearing on Premera's website states and represents in relevant part as follows:

> **THE PRIVACY OF YOUR MEDICAL AND FINANCIAL INFORMATION IS VERY IMPORTANT TO US.**
>
> At Premera Blue Cross, we are committed to maintaining the confidentiality of your medical and financial information, which we refer to as your "personal information," regardless of format: oral, written, or electronic. This Notice of Privacy Practices informs you about how we may collect, use and disclose your personal information and your rights regarding that information.
>
> * * *

[6] Notice of Privacy Rights, PREMERA, https://www.premera.com/wa/visitor/privacy-policy/.

> **OUR RESPONSIBILITIES TO PROTECT YOUR PERSONAL INFORMATION**
>
> Under both the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act, Premera Blue Cross must take measures to protect the privacy of your personal information. In addition, other state and federal privacy laws may provide additional privacy protection. Examples of your personal information include your name, Social Security number, address, telephone number, account number, employment, medical history, health records, claims information, etc.
>
> We protect your personal information in a variety of ways. For example, we authorize access to your personal information by our employees and business associates only to the extent necessary to conduct our business of serving you, such as paying your claims. We take steps to secure our buildings and electronic systems from unauthorized access. We train our employees on our written confidentiality policy and procedures and employees are subject to discipline if they violate them. Our privacy policy and practices apply equally to personal information about current and former members; we will protect the privacy of your information even if you no longer maintain coverage through us.[7]

32. In the Premera Blue Cross Code of Conduct 2014 published on Premera's primary website, the Company stated and represented in relevant part as follows:

> We are committed to complying with federal and state privacy laws, including the HIPAA privacy regulations, that protect financial and health information of our customers. We use the following privacy principles to guide our actions:
>
> Customers - Customers should enjoy the full array of privacy protections afforded to them by law and routinely granted by their providers. This is a values-based approach whereby we are focused on two core values: Customer Care and Integrity.
>
> * * *
>
> We are committed to ensuring the security of our facilities and electronic systems to prevent unauthorized access to Premera's and our customers' personal protected information (PPI).

[7] *Id.*

> We are expected to be aware of and follow established corporate policies, processes and procedures that are designed to secure our buildings and electronic systems. We are all responsible for maintaining the security of our campuses and buildings.

33. Premera's statements and representations promising Premera customers and consumers that its IT systems were secure, as stated and represented in Premera's published privacy policies and in Premera's other public representations, falsely inflated the price of Premera insurance, allowing Premera and/or its affiliates to charge higher premiums for insurance. In purchasing Premera health insurance, Plaintiffs and the proposed Class Members paid for insurance to be provided by an insurer which was taking affirmative and commercially reasonable measures to protect their private banking and healthcare information and actively preventing its disclosure and unauthorized access.

34. As described below, Premera failed to fulfill its promises and also failed to take reasonable steps to safeguard the personal health, identification, and financial information of Plaintiffs and the proposed Class Members.

II. PREMERA IGNORED WARNINGS BEFORE THE BREACH

35. In April 2014, as reported in The Seattle Times, federal auditors from the U.S. Office of Personnel Management ("OPM") had warned Premera that its IT security procedures were inadequate.[8]

36. Premera is one of the insurance carriers participating in the Federal Employees Health Benefits Program and thus Premera's IT applications that manage claims from federal workers were audited.[9]

---

[8] Baker, *supra* note 3.

[9] *Id*.

37. The auditors conducted vulnerability scans and determined Premera was not "implementing critical patches and other software updates in a timely manner" and that the failure "to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive data could be breached."[10]

38. Additional findings from the audit include, but are not limited to, the following: (1) software applications so old that they were no longer supported by the vendor and had known security problems; (2) servers containing "insecure configurations" that can grant hackers access to sensitive information; and (3) the need to implement better physical controls to prevent unauthorized access to its data center. Based upon its findings, OPM gave ten recommendations to Premera to fix the identified IT problems.[11]

39. In response to the audit findings, Premera claimed it would start using procedures to properly update its software. However, Premera also claimed it was in compliance with regard to the management of its "critical security patches," despite OPM's vulnerability scans indicating Premera was not in compliance.[12]

40. Premera's failure to timely implement OPM's recommendations could have prevented the harm done to Plaintiff and members of the Class.

III. THE BREACH AND PREMERA'S SECURITY PRACTICES

41. The personal health, identification, and financial information of Plaintiffs and the proposed Class members, while under the control of Defendant, was accessed without Plaintiffs or proposed Class members' authorization. The exact details regarding the mechanics of the Data Breach are mostly unknown and will be further determined during discovery.

---

10 *Id.*
11 *Id.*
12 *Id.*

42. On March 17, 2015, Premera announced that its information technology systems had been hacked, resulting in the improper disclosure of personal health, identification, and financial information of approximately 11 million current and former customers. Premera also stated that the hackers may have gained access to information dating as far back as 2002.

43. The personal health, identification, and financial information of Plaintiffs and the members of the Class, including, but not necessarily limited to, full legal names, birth dates, Social Security numbers, medical identification numbers, health histories, street addresses, email addresses, employment information, income data, and other personal information was improperly accessed without the authorization of Plaintiffs and the members of the Class while that information was in the custody and control of Premera.

44. Premera has publicly stated that it discovered the Data Breach on January 29, 2015, and then announced it on March 17, 2015. However, the cyberattack had occurred eight months prior to Premera announcing the attack. In other words, Premera did not realize for months that its IT system had been compromised.

45. The data breach affected Premera Blue Cross, Premera Blue Cross Blue Shield of Alaska, and Premera's affiliated companies, Vivacity and Connexion Insurance Solutions Inc. The Data Breach also affected members of other Blue Cross Blue Shield plans who sought treatment in Washington or Alaska. Individuals who do business with Premera and provided Premera with their email address, personal bank account number or social security number were also affected.

IV. PREMERA'S CONDUCT VIOLATED INDUSTRY STANDARDS AND OTHER APPLICABLE STATUTES AND GUIDELINES

46. The 2013 Identity Fraud Report released by Javelin Strategy & Research reports that in 2012 identity fraud incidents increased by more than one million victims, and fraudsters

stole nearly $21 billion in actual theft. The study found 12.6 million victims of identity fraud in the United States in the past year, which equates to 1 victim every 3 seconds. The report also found that nearly 1 in 4 data breach letter recipients became a victim of identity theft, with breaches involving Social Security numbers to be the most damaging: consumers who had their Social Security number compromised in a data breach were 5 times more likely to be a victim than an average consumer.

47. Given the well-publicized increases in data thefts, Defendant had a duty to protect the private, highly sensitive, confidential personal health, identification, and financial information of Plaintiffs and the proposed Class members.

48. Indeed, Defendant was statutorily obligated to adequately protect the information in question because it is protected information under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 29 U.S.C.A. §§ 1181 *et seq.*, because it includes patient names, addresses, birthdates, telephone numbers and Social Security numbers.

49. HIPAA required Defendant to "reasonably protect" the information from "any intentional or unintentional use or disclosure." 45 C.F.R. § 164.530(c)(1)(2)(i). Federal regulations also required Defendant to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." *Id.* at § 164.530(c)(1).

50. Defendant violated HIPAA by failing to maintain the confidentiality of Plaintiffs' and the proposed Class members' protected personal health, identification and financial information.

51. In addition to failing to comply with basic rules of conduct and HIPAA, Defendant failed to employ reasonable and industry standard safeguards and procedures that

would have prevented vulnerabilities in its information technology systems from being exploited by hackers.

52. To assist companies in protecting the security of sensitive personal and financial information, the Federal Trade Commission ("FTC") has issued a publication entitled "Protecting Personal Information: A Guide for Business" (the "FTC Report"). In this publication, the FTC provides guidelines for businesses on how to develop a "sound data security plan" to protect against crimes of identity theft.

53. To protect the personal sensitive information in their files, the FTC Report instructs businesses to follow the following guidelines:

a) Keep inventory of all computers and laptops where the company stores sensitive data;

b) Do not collect personal information if there is no legitimate business need. If there is a legitimate business need, only keep the information as long as necessary;

c) Use Social Security numbers only for required and lawful purposes and do not store these numbers unnecessarily, such as for an employee or customer identification number;

d) Encrypt the personal information, particularly if the sensitive information is shipped to outside carriers or contractors. In addition, the business should keep an inventory of all the information it ships;

e) Do not store sensitive computer data on any computer with an Internet connection or access unless it is essential for conducting the business;

f) Control access to sensitive information by requiring that employees use "strong" passwords; and

g) Implement information disposal practices that are reasonable and appropriate to prevent unauthorized access to personally identifying information.

54. Defendant failed to employ these and other basic safeguards and, as a result of that failure, unauthorized third parties were able to bypass Defendant's inadequate security

measures and successfully access personal health, identification, and financial information of Plaintiffs and the proposed Class members.

55. As described above, Defendant violated federal guidelines and failed to meet current data security industry standards by failing to ensure adequate security over Plaintiffs' and the proposed Class members' personal health, identification, and financial information and by failing to retain Plaintiffs' and the proposed Class members' personal health, identification, and financial information in a secure and safe manner.

56. Premera's failure to follow both basic and best data security practices has caused direct harm and injury to Plaintiffs and the Class.

V. PREMERA IMPROPERLY DELAYED NOTIFYING VICTIMS OF THE DATA BREACH

57. Premera discovered the Data Breach on January 29, 2015, and publicly announced the Data Breach on March 17, 2015, and declared that it was only beginning to mail letters to the victims of the Data Breach.

58. Mike Kreidler, Washington State Insurance Commissioner, stated in a news release "I remain seriously concerned at the amount of time it took Premera to notify its policyholders of the breach."[13]

59. On information and belief, no law enforcement agency instructed Premera to delay notification to Plaintiffs and the members of the Class.

60. Additionally, Premera continued to accept monies from Plaintiffs and members of the Class when Premera had actual knowledge its IT systems were unsecure and the Data breach had occurred.

---

[13] News Release, *Washington to lead multi-state investigation of Premera,* WASHINGTON STATE OFFICE OF THE INSURANCE COMMISSIONER (March 24, 2015), http://www.insurance.wa.gov/about-oic/news-media/news-releases/2015/03-24-2015.html.

61. Specifically, the failure to notify the Plaintiffs and the Class that its IT systems were unsecure and, in fact, had been breached, prevented Plaintiffs and the members of the Class from avoiding and/or otherwise mitigating their damages. Plaintiffs and members of the Class were denied the opportunity to avoid providing further information to Premera, denied the opportunity to avoid using Premera's services, and denied the opportunity to contact their providers to protect their private information.

VI. THE CLASS WAS DAMAGED BY PREMERA'S CONDUCT AND/OR INACTION

62. Premera's failure to maintain reasonable and adequate security procedures to protect against the theft of Plaintiffs' and the members of the Class's personal health, identification, and financial information has also put members of the Class at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse. As Paul Stephens, Director of Policy and Advocacy at the Privacy Rights Clearinghouse in San Diego, said, the wide array of types of personal information opens up more possibilities for intrusions and indicates that another attack is imminent: "'You essentially have the keys to the kingdom to commit any type of identity theft . . . . The information can be used not only to establish new credit accounts but also potentially penetrate existing accounts at financial institutions or a stock brokerage. The scope of the information involved is incredible.'"[14]

63. Significantly, Premera's offer to provide free credit monitoring to impacted Class members will not stop medical identity theft as a result of the Data Breach. Because the Data Breach involved compromise of medical identification, numbers on customer health insurance cards, and other personal information, "[c]riminals can use those numbers at hospitals,

[14] Chad Terhune, *Anthem Hack Exposes Data on 80 Million; Experts Warn of Identity Theft*, L.A. TIMES, http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html#page=1.

emergency rooms and pharmacies to receive care and prescriptions, racking up charges and wrecking victims' medical records." As Bob Gregg, CEO of ID Experts explained, "[i]t's like an unlimited credit card that gets you 'free' access to expensive services and drugs . . . . Everyone thinks about credit cards and bank accounts, but medical identity theft can be much more damaging and extremely hard to fix." Any medical care received using fraudulent medical identification gets added to the health records attached to the identification number, and may take months or years to surface.[15]

64. Accordingly, Premera's failure to protect personal health, identification, and financial information may also have medical implications for Class members for years to come. As NBC News reported, "[i]magine an unwitting medical ID theft victim who is rushed to the hospital for emergency gallbladder removal, but the patient's record shows the gallbladder was removed last year. That could cause confusion for the healthcare providers and serious delays in treatment, as could incorrect information about blood types or possible drug interactions."[16]

65. Moreover, although Premera admits the importance of monitoring the credit of the class going forward, it is only providing two years of free credit monitoring. Premera's own website includes the following in the FAQ section:

> **What is Premera doing to protect me after this incident?**
>
> We're offering two years free credit monitoring and identity theft protection services to anyone affected by this incident. We worked with one of the world's leading cybersecurity firms, Mandiant, to investigate the attack and remove the infection from our systems. We've taken

[15] Julianne Pepitone, *Anthem Hack: Credit Monitoring Won't Catch Medical Identity Theft*, NBC NEWS (Feb. 5, 2015), http://www.nbcnews.com/tech/security/anthem-hack-credit-monitoring-wont-catch-medical-identity-theft-n300836.

[16] *Id.*

> additional actions to strengthen and enhance the security of our IT systems moving forward. We're also coordinating with the FBI as they conduct their own investigation into the attack.[17]

66. Plaintiffs and members of the Class will incur additional expenses that will not be reimbursed by Defendant for credit monitoring services after the two years of services provided for by Defendant. Plaintiffs and members of the Class will be forced to pay for services or face additional exposure and risk if they choose to proceed unmonitored.

67. In addition to the ongoing and continued damage to the Class as a result of their increased and continued exposure to identity and medical theft as a result of the Data Breach, Plaintiffs and the members of the Class have been harmed in that they paid for protections and services they did not receive when being provided healthcare by Defendant. A portion of the consideration paid for healthcare by Plaintiffs and the proposed Class members was accepted by Defendant and was allocated to protecting and securing Plaintiffs' and the proposed Class members' personal health, identification, and financial information and ensuring HIPAA compliance. This allocation was made for the purpose of offering patients and consumers, such as Plaintiffs and the proposed Class members, added value to the health care services provided by agreeing to protect their protected personal health, identification and financial information.

68. Because of the real threat of immediate harm, the intrinsic value of the stolen information itself and the failure of Defendant to provide Plaintiffs and the proposed Class with the benefit of the bargain made when obtaining healthcare from Premera, Plaintiffs and members of the Class have suffered an immediate and present financial injury as well as an injury to their privacy and possessory interests in their sensitive personal information. All of these damages

---

[17] Premera FAQ, http://www.premeraupdate.com/faqs/.

flow directly from Defendant's negligent failure to safeguard this sensitive information as well as the breach of its agreement to do the same.

69. Moreover, Plaintiffs and the proposed Class members have been or are at an increased and imminent risk of becoming victims of identity theft crimes, fraud and abuse, and have been forced to spend considerable time and money to protect themselves – and face years of constant surveillance of their financial and medical records, monitoring, loss of rights, and potential medical problems, among other harms – as a result of Premera's conduct in failing to adequately protect their personal health, identification and financial information.

70. In addition to these losses, Plaintiffs and the Class were also harmed by Defendant's inexcusable failure to provide timely notification to Plaintiffs and proposed Class members of the Data Breach. That failure deprived Plaintiffs and proposed Class members of critical time to protect themselves from, among other injuries, identity theft.

CLASS ACTION ALLEGATIONS

71. Plaintiffs bring this action on behalf of themselves and on behalf all other persons similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

72. The Nationwide Class is defined as follows:

> All persons whose personal health, identification, and financial information was contained in or on the Premera computer system and whose personal health, identification, or financial information was stolen or otherwise misappropriated as a result of the Data Breach that was announced on or about March 17, 2015 (collectively, the "Class").
>
> Excluded from the Class are Defendant; officers and directors of Defendant; any entity in which Defendant has a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendant, and; the Court and its officers, employees, and relatives.

73. Plaintiffs also seek to certify a Subclass of the Class for Washington residents.

74. The Washington Subclass is defined as follows:

> All residents of the State of Washington whose personal health, identification, and financial information was contained in or on the Premera computer system and whose personal health, identification, or financial information was stolen or otherwise misappropriated as a result of the Data Breach that was announced on or about March 17, 2015. (collectively, the "Subclass").

75. Plaintiffs are members of the Class and Subclass they seek to represent.

76. This action satisfies the procedural requirements set forth in Rule 23 of the Federal Rules of Civil Procedure.

77. The conduct of Defendant has caused injury to members of the Class.

78. The Class is so numerous that joinder of all members is impracticable, as approximately 11 million individuals' personal health, identification or financial information may have been compromised in the data breach that Premera first disclosed on March 17, 2015.

79. The members of the Class are readily ascertainable, as they can be identified by records maintained by Defendant. Notice can be provided by means permissible under the Federal Rules of Civil Procedure.

80. There are substantial questions of law and fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Premera failed to provide adequate security and or protection for its computer systems containing Plaintiffs' and members of the potential Class's personal health, identification or financial information;

b. Whether Premera's conduct resulted in the unauthorized breach of its computer systems containing Plaintiffs' and members of the potential Class's personal health, identification or financial information;

c. Whether Premera improperly retained Plaintiffs' and members of the potential Class's personal health, identification or financial information;

d. Whether Premera disclosed (or directly or indirectly caused to be disclosed) private personal health, identification or financial information of Plaintiffs and members of the potential Class;

e. Whether Premera owed a legal and/or contractual duty to Plaintiffs and members of the potential Class to use reasonable care in connection with its use and retention of personal health, identification or financial information;

f. Whether Premera breached its duties to exercise reasonable care in obtaining, using, retaining, and safeguarding Plaintiffs' and members of the potential Class's personal health, identification or financial information;

g. Whether Premera was negligent;

h. Whether Premera's breach of its duties proximately caused damages to Plaintiffs and the other members of the Class;

i. Whether Premera is in breach of contract;

j. Whether Premera violated the Washington Consumer Protection Act and other relevant consumer protection statutes;

k. Whether Plaintiffs and members of the Class have suffered damages, including but not limited to, an increased risk of identity theft as a result of Premera's failure to protect Plaintiffs' and the Class members' personal health, identification or financial information; and

l. Whether Plaintiffs and other members of the Class are entitled to compensation, damages, and/or other relief as a result of the breach of duties alleged herein.

81. Plaintiffs' claims are typical of the claims of all members of the Class. The same events and conduct that give rise to Plaintiffs' claims and legal theories also give rise to the claims and legal theories of the Class. Specifically, Plaintiffs' and members of the Class's

claims arise from Premera's failure to install and maintain reasonable security measures to protect Plaintiffs' and members of the Class's personal health, identification and financial information.

82. The conduct of Premera has caused injury and/or imminent threat of injury to Plaintiffs and members of the Class.

83. Plaintiffs are members of the putative Class, possess the same interests, and suffered the same injuries as Class members, making their interests coextensive with those of the Class. The interests of Plaintiffs and the Class are aligned so that the motive and inducement to protect and preserve these interests are the same for each.

84. Premera has acted and refused to act on grounds generally applicable to the Class described herein.

85. Prosecuting separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Premera.

86. Plaintiffs will fairly and adequately represent the interests of the Class. There are no disabling conflicts of interest between Plaintiffs and the Class.

87. Plaintiffs are represented by experienced counsel who are qualified to litigate this case. The lawsuit will be capably and vigorously pursued by Plaintiffs and their counsel.

88. A class action is superior to other available methods for a fair and efficient adjudication of this controversy since joinder of all members of the Class is impracticable. Furthermore, the damages suffered by individual class members may be relatively small in comparison with the expense and burden associated with individual litigation, which make it impossible for them to individually redress the harm done to them. Proceeding as a class action

will permit an orderly and expeditious administration of the claims of Class members, will foster economies of time, effort, and expense and will ensure uniformity of decision. There will be no difficulty in the management of this litigation as a class action.

COUNT I
NEGLIGENCE

89. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

90. Premera had a duty to exercise reasonable care to protect and secure Plaintiffs' and the members of the Class's personal health, identification, and financial information in its possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This highly confidential personal health, identification, and financial information includes but is not limited to full legal names, birth dates, Social Security numbers, medical identification numbers, health histories, street addresses, telephone numbers, email addresses, bank account information, and other personal information.

91. Premera's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiffs' and the members of the Class's personal health, identification, and financial information in their possession was adequately secured and protected and was retained only for legitimate purposes and with adequate storage, retention, and disposal policies.

92. Premera further had a duty to implement processes that would detect a breach of its security systems in a timely manner.

93. In light of the special relationship between Plaintiffs and members of the Class and Premera, whereby Premera required Plaintiffs and members of the Class to provide highly sensitive confidential personal health, identification, and financial information as a condition of

application, availability of health insurance, and employment, Premera undertook a duty of care to ensure the security of such information.

94. Premera also knew or should have known that hackers would target the highly confidential personal health, identification, and financial information of Plaintiffs and the members of the Class. Indeed, countless data breaches in just the past year have exploited similarly lax security controls to gain access to company-wide databases. Moreover, a number of these data breaches have targeted medical companies/institutions and the personal health, identification, and financial information of their patients/customers. As a result, it was quite clear, or at least reasonably foreseeable, that the information of Plaintiffs and the members of the Class was a high value target to criminal third parties. Premera thus had a duty to take reasonable steps in protecting this information.

95. Through its acts or omissions, Premera breached its duty to use reasonable care to protect and secure Plaintiffs' and the members of the Class's personal health, identification, and financial information in its possession or control. Premera breached its duty by failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and members of the Class's personal health, identification and financial information, failing to adequately monitor the security of its network, allowing unauthorized access to Plaintiffs' and the members of the Class's personal health, identification and financial information, and failing to recognize in a timely manner that Plaintiffs' and members of the Class's personal health, identification, and financial information had been compromised.

96. Premera's failure to comply with widespread industry standards relating to data security further evinces Premera's negligence in failing to exercise reasonable care in

safeguarding and protecting Plaintiffs' and the members of the Class's personal health, identification, and financial information in its possession or control.

97. But for Premera's wrongful and negligent breach of the duties owed to Plaintiffs and the members of the Class, the Data Breach would not have occurred and Plaintiffs' and the members of the Class's personal health, identification, and financial information would not have been compromised.

98. The injury and harm suffered by Plaintiffs and the members of the Class was the reasonably foreseeable and probable result of Premera's failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the members of the Class's personal health, identification, and financial information in its possession or control. Premera knew or should have known that its systems and technologies for processing and securing Plaintiffs' and members of the Class's personal health, identification, and financial information had significant vulnerabilities.

99. As a result of Premera's negligence, Plaintiffs and the members of the Class have incurred damages, including, but not limited to, the increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse.

COUNT II
BREACH OF IMPLIED CONTRACT

100. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

101. When Premera required Plaintiffs and the members of the Class to supply their personal health, identification and financial information, Premera entered into implied contracts with Plaintiffs and the members of the Class to protect the security of such information.

102. Such implied contracts arose from the course of conduct between Plaintiffs and the members of the Class and Premera.

103. The implied contracts required Premera to safeguard and protect Plaintiffs' and the members of the Class's personal health, identification, and financial information from being accessed, compromised, and/or stolen.

104. Premera did not safeguard or protect Plaintiffs' and the Class members' personal health, identification, and financial information from being accessed, compromised, and/or stolen. Premera did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiffs' and the Class members' personal health, identification and financial information.

105. Because Premera failed to safeguard and/or protect Plaintiffs' and the Class members' personal health, identification, and financial information from being accessed, compromised or stolen, Defendant breached its contracts with Plaintiffs and the members of the Class.

106. Plaintiffs and the members of the Class would not have provided and entrusted their personal health, identification, and financial information to Premera in order to purchase Premera services in the absence of the implied contract between Plaintiffs and the Class and Premera.

107. Plaintiffs and the members of the Class have suffered and will continue to suffer damages as the result of Premera's breach.

COUNT III
NEGLIGENCE *PER SE*

108. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

109. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Premera had a duty to protect the personal and financial information of its customers.

110. Premera violated the Gramm-Leach-Bliley Act by failing to protect Plaintiffs' and Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with data security standards, card association standards, statutes and/or other regulations to protect such personal and financial information.

111. Plaintiffs and the members of the class are within the sphere of individuals Congress intended to be protected by the Gramm-Leach-Bliley Act.

112. Premera's failure to comply with the Gramm-Leach-Bliley Act constitutes negligence *per se*.

113. HIPAA was designed to protect the privacy of personal medical information by limiting its disclosure.

114. HIPAA seeks to protect the privacy of protected patient personal health, identification, and financial information by prohibiting any voluntary or involuntary use or disclosure of such data in violation of the directives set out in the statute and its regulations.

115. It is common practice for Washington health care providers, as well as health care providers nationwide, to follow the procedures required under HIPAA in rendering services to their patients.

116. As described above, Defendant violated HIPAA by failing to maintain the confidentiality of its protected patient personal health, identification and financial information.

117. Plaintiffs and the proposed Class members have suffered harm, including but not limited to expenses for credit monitoring, loss of privacy, and other economic and non-economic harm, as well as an being placed at an increased and imminent risk of becoming victims of

identity theft crimes, fraud, and abuse as a result of Defendant's violation.

118. Plaintiffs and the proposed Class members are persons whom Congress intended to be protected by HIPAA.

119. Defendant is a HIPAA-covered entity.

120. The personal health, identification, and financial information of Plaintiffs and the Class members are the types of records HIPAA was created to protect.

121. The injuries suffered by Plaintiffs and the proposed Class members were directly and proximately caused by Defendant's violation of HIPAA.

122. Defendant's violation of HIPAA thus constitutes negligence *per se* and Plaintiffs and the proposed Class members are entitled to recover damages in an amount to be proven at trial.

COUNT IV
UNJUST ENRICHMENT

123. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

124. Plaintiffs bring Count IV in the alternative to their claim for breach of contract.

125. Defendant received payment from Plaintiffs and the proposed Class members to perform services that included protecting Plaintiffs' and the proposed Class members' personal health, identification and financial information.

126. Defendant did not protect Plaintiffs' and the proposed Class members' personal health, identification and financial information, but retained Plaintiffs' and the proposed Class members' payments.

127. Defendant retained the benefits of Plaintiffs' and the proposed Class members' payments under circumstances which rendered it inequitable and unjust for Defendant to retain

such benefits without paying for their value.

128. Defendant has knowledge of said benefits.

129. As a result, Plaintiffs and the proposed Class members have been proximately harmed and/or injured as described herein.

COUNT V
FAILURE TO TIMELY DISCLOSE BREACH UNDER RCW 19.255.010

130. Plaintiffs incorporate and re-allege each and every allegation contained above as if fully set forth herein.

131. Premera is a business that conducts business in Washington and owns or licenses computerized data that includes personal information, as defined under RCW 19.255.010.

132. On or around May 5, 2014, unauthorized individuals gained access to personal and financial information stored in Premera's computer system.

133. Premera knew or should have known that the breach occurred, but due to its own negligent monitoring of its information systems, it did not discover the breach until January 29, 2015.

134. Premera then failed to immediately notify the persons whose data was breached until March 17, 2015.

135. Premera's failure to detect and disclose the breach constituted an unreasonable delay.

136. Plaintiffs and the Class have suffered damages as a direct and proximate result of Premera's failure to provide reasonably prompt disclosure of the data breach.

COUNT VI
VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT

137. Plaintiffs incorporate and re-allege each and every allegation contained above as

if fully set forth herein.

138. This claim is brought pursuant to the Washington Consumer Protection Act, RCW Ch. 19.86 (the "CPA").

139. The CPA prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce.

140. Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of healthcare policies to consumers, including Plaintiffs and members of the Class.

141. Defendant is engaged in, and its acts and omissions affect trade and commerce.

142. Defendant's acts, practices, and omissions complained of herein were done in the course of Premera's business throughout the United States, including the State of Washington.

143. Defendant's conduct as alleged in the Complaint, including without limitation, Premera's failure to maintain adequate IT systems and data security practices to safeguard customers' personal health, identification and financial information, Premera's failure to disclose in a timely and accurate manner the material fact of the data security breach, constitutes unfair methods of competition and unfair and/or deceptive acts or practices within the meaning of the CPA.

144. Defendant represented that its provision of insurance and sale of insurance policies were secure services/products and that administrative staff and procedures were in place to protect any information used in the provision and sale of these services/products. However, Defendant knew that this was not the case as Defendant utilized sub-standard data security during the handling and storage of the personal information of Plaintiffs and members of the Class.

145. The deceptive and unconscionable actions of Defendant were done in the course of business, trade, and commerce. Further, a negative impact on the public interest was caused by Defendant's conduct.

146. Plaintiffs and members of the Class have suffered damages, as a result of Defendant's unfair acts and/or deceptive practices in the form of expenses for credit monitoring, lost work time, anxiety, emotional distress, loss of privacy, and other economic and non-economic harm, as well as being placed at an increased and imminent risk of becoming victims of identity theft crimes, fraud, and abuse.

147. Because Premera violated the CPA, Plaintiffs and members of the Class are entitled to damages pursuant to RCW § 19.86.090, up to three times the value of the actual damages sustained, and attorneys' fees and costs.

148. Plaintiffs have provided notice of this action and a copy of this Complaint to the Washington State Attorney General pursuant to RCW § 19.86.095.

PRAYER FOR RELIEF

149. Plaintiffs request that this Court enter judgment against Defendant and in favor of Plaintiffs and the proposed Class members and award the following relief:

A) That this action be certified as a Class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiffs as the representatives of the Class and Plaintiffs' counsel as counsel for the Class;

B) Monetary damages;

C) Injunctive relief, including but not limited to the provision of credit monitoring services for Plaintiffs and the proposed Class members for a period of at least 25 years, the provision of bank monitoring services for Plaintiffs and the proposed Class members for a period

of at least 25 years, the provision of credit restoration services for Plaintiffs and the proposed Class members for a period of at least 25 years, and the provision of identity theft insurance for Plaintiffs and the proposed Class members for a period of at least 25 years;

D) Reasonable attorneys' fees and expenses, including those related to experts and consultants;

E) Costs;

F) Pre and post judgment interest;

G) Such other relief as this Court may deem just and proper.

JURY DEMAND

Pursuant to Fed. R. Civ. P 38(b), Plaintiffs, on behalf of themselves and on behalf of the Class they seek to represent, hereby demand a trial by jury on all causes of action asserted in this action so triable.

Dated: June 8, 2015

By: */s/ Deborah M. Nelson*

Deborah M. Nelson, WSBA #23087
Jeffrey D. Boyd, WSBA #41620
NELSON BOYD, PLLC
411 University Street
Suite 1200
Seattle, WA 98101
206.971.7601
nelson@nelsonboydlaw.com
boyd@nelsonboydlaw.com